

UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Fayetteville Division

US DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FILED

NOV 12 2019

DOUGLAS F. YOUNG, Clerk
By
Deputy Clerk

In the Matter of the Search of)
iPhone 8 Plus bearing)
Identification number FD5W22CZJCLY)

Case No. 5:19cm122

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe property to be searched and give its location*): **See Attachment A**

located in the Western District of Arkansas, there is now concealed (*identify the person or describe the property to be seized*): **See Attachment B**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

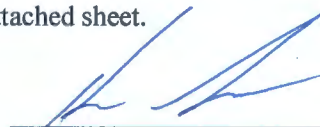
18 U.S.C. § 2422(b)

Attempted Online Enticement of a Minor

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Kevin Sears, HSI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: November 12, 2019


Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, Chief United States Magistrate Judge
Printed name and title

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS

:
:
:
:
:

ss. AFFIDAVIT

COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, Kevin Sears, a TFO with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Task Force Officer (TFO) with the Department of Homeland Security, Homeland Security Investigations ("HSI"), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with Washington County Sheriff's Office since January, 2007. As part of my daily duties as an HSI TFO, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. This Affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

2. This Affidavit is being submitted in support of an application for a search warrant for electronic devices described as being an iPhone 8 plus bearing identification number

FD5W22CZJCLY, also referred to as “**SUBJECT ITEM**”, located and seized from Jay THOMPSON’s person at the time of his encounter and state arrest in Fayetteville, Arkansas, which is now being stored in evidence at the Homeland Security Office in Fayetteville, Arkansas. As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant.

Statutory Authority

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2422(b) – Attempted Online Enticement of a Minor, making it a crime for a person to use the internet or any other means, which affects interstate commerce, attempt to knowingly persuade, induce, entice and coerce a person who has not attained the age of 18 years to be caused to engage in a criminal sex act. Arkansas Code Annotated 5-14-103(a)(3)(A), Rape, a Class Y felony, makes it a criminal offense for a person to engage in sexual intercourse or deviate sexual activity with another person who is less than fourteen (14) years of age. Deviate sexual activity is defined in Arkansas Code Annotated 5-14-101 as “any act of sexual gratification involving the penetration, however slight, of the anus or mouth of a person by the penis of another person; or the penetration, however slight, of the labia majora or anus of a person by any body member or foreign instrument manipulated by another person.”

4. Under 18 U.S.C. Section 2422(b), it is a federal crime for any person to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so. Further, under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2422(b), shall forfeit to the United States such

person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

**BACKGROUND REGARDING COMPUTER/ELECTRONIC DEVICES
AND THE INTERNET**

5. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

- a. Cell phones and more advanced devices known as "smart phones" function the same as computers and can run computer software and applications, create and edit files, access the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used by child pornographers to send, receive, store, and produce images depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs and other data.
- b. Computer technology, including mobile smart or cell phones, and the Internet have revolutionized the manner in which persons who have a sexual interest in children can communicate. The Internet affords individuals several different venues for meeting each other, meeting children and their parents, obtaining, viewing and trading child pornography in a relatively secure, and anonymous fashion.
- c. Computers, including cell phones, serve five functions in connection with child exploitation: production of child pornography, communication, distribution, storage, and social networking. In addition, new technologies are developing

allowing average computer users avenues to mask their IP addresses for more private Internet browsing sessions.

- d. Through the Internet, electronic contact can be made to literally millions of computers around the world using any of their devices.
- e. As with most digital technology, communications made from a computer or smart phone are often saved or stored on that device. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is,

in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's type of device, operating system, storage capacity, and computer habits.

Background Regarding Craigslist

6. Based on my knowledge and experience and information obtained from other law enforcement personnel with training and experience in this area, the following is known about Craigslist:

- a. Craigslist is a classified advertisement website with sections devoted to jobs, housing, for sale, items wanted, services, community service, gigs, resumes, and discussion forums.
- b. The website began services in 1995 as an email distribution list to friends, featuring local events in California. It then became a web-based service in 1996 and expanded into other classified categories. Craigslist started expanding in 2000, and now covers 70 countries.
- c. The website serves more than approximately 20 billion page views per month, putting it 72nd place overall among websites in the United States with more than 49.4 million unique monthly visitors in the United States alone.

- d. Over the years, Craigslist became a very popular online destination in arranging personal dates and sexual encounters through their "Personals" section. In March 2018, Craigslist discontinued the section in response to the passing of the Stop Enabling Sex Trafficking Act by the United States Congress.
- e. Craigslist has a user flagging system to quickly identify illegal and inappropriate postings. Users may flag postings they believe to be in violation of Craigslist guidelines. Flagging does not require account login or registration, and can be done anonymously by anyone.

Summary of the Investigation to Date

7. Beginning in September 2019, the HSI Internet Crimes Against Children (ICAC) Task Force and Arkansas State Police with assistance from local law enforcement agencies, set up an operation to target online predators during the 2019 Bikes, Blues and BBQ Rally in Northwest Arkansas. As a part of the operation, undercover law enforcement agents put out multiple advertisements on online websites and mobile applications or "apps."

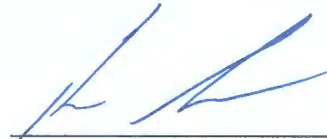
8. On or about September 25, 2019, THOMPSON responded to an undercover Craigslist advertisement where an undercover law enforcement officer was representing himself/herself to be a thirteen (13) year old minor female. Between September 25 and September 26, 2019, the two communicated back and forth. THOMPSON engaged in several emails with the believed minor female. The undercover then supplied THOMPSON with a phone number to communicate over text messages. THOMPSON continued to communicate over text messages utilizing phone number 479-957-XXXX where he discussed specific details of performing sexual activities and arranged a meeting for a sexual encounter. On September 26, 2019, at approximately 1600 hours, THOMPSON was encountered as he arrived at the prearranged meeting location discussed with the believed thirteen (13) year old minor female for the sexual encounter. At the time of his arrest for violations of Arkansas state laws, THOMPSON was found to be in possession

of an Apple iPhone 8 plus bearing identification number FD5W22CZJCLY (**SUBJECT ITEM**).

9. During a post-Miranda interview, THOMPSON admitted to being the individual responsible for communicating with the believed minor female. The **SUBJECT ITEM**, which was the only electronic device located on THOMPSON at the time of his arrest, is believed to be the cellular telephone utilized to communicate with the undercover agent.

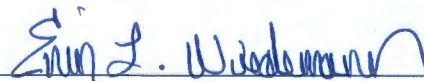
Conclusion

10. Based on the foregoing information, probable cause exists to believe there is located on an iPhone 8 plus bearing identification number FD5W22CZJCLY, the **SUBJECT ITEM**, evidence of violations of Title 18, United States Code, Section 2422(b), et seq. Your Affiant prays upon his honorable court to issue a search warrant for the **SUBJECT ITEM** for the item set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Section 2422(b), et seq.



Kevin Sears, Task Force Officer
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 12th day of November, 2019.



Honorable Erin L. Wiedemann
Chief United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

IPhone 8 plus bearing identification number FD5W22CZJCLY seized from Jay Thompson on
September 26, 2019

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

Evidence of violations of 18 U.S.C. Section 2422(b) including the following:

- a. Information or correspondence pertaining to the sexual exploitation of minors or solicitation of such for sexual activity, including any and all information such as e-mail, chat logs, text messages, etc. related to the online enticement of a minor, including but not limited to:
 - i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, text messages, establishing possession, identity of individuals (including Contact lists), access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of transfer or attempted transfer of obscene material to a minor;
 - ii. Any and all chat log, text messages, email, or any type of communication in any form that is related to the transfer or attempted transfer of obscene material to a minor
 - a. Including messages sent to individuals discussing the sexual assault or desire to sexually assault minors or discussion of online posts regarding images of child pornography.
 - b. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or send the minor pictures and or videos of sexually explicit conduct.
- c. Records evidencing ownership of the items seized, including in and all lists of names, telephone numbers, addresses and contacts, and the content of voice mails and text messages and internet based applications including but not limited to:
 - i. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.
 - ii. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device